REMARKS

Claims 1, 3-18, 20-29 and 31-33 are currently pending in the subject application and are presently under consideration. Claims 1, 27 and 28 have been amended and claim 33 has been cancelled as shown on pages 2-6 of the Reply. The below comments present in greater detail distinctive features of applicants' claimed invention over the cited art that were conveyed to the Examiner over the telephone on November 2, 2007.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 3-16, 27-29, 31 and 33 Under 35 U.S.C. §101

Claims 1, 3-16, 27-29, 31 and 33 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. This rejection should be withdrawn for at least the following reasons. The subject claims are directed to statutory subject matter.

In particular, the Examiner states that claimed limitations merely disclose software implemented elements or data structures along with their intended uses. Claim 1 recites a computer implemented system with processor executable components comprising a wrapper that packages credentials and a pass-phase employed in connection with generation of the wrapper,. Claim 27 recites facilitating a security relationship between partners, comprising computer implemented means for storing and means for transmitting which would be associated with hardware devices. As such the claimed subject matter produces a useful, concrete tangible result while reciting statutory subject matter. Accordingly, it is requested that this rejection should be withdrawn.

II. Rejection of Claims 28-29 and 33 Under 35 U.S.C §112

Claims 28-29 and 33 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the written description requirement. Independent claim 28 has been amended herein to cure the minor informalities. Independent claims 33 stands cancelled herein. Accordingly, it is requested that this rejection be withdrawn.

III. Rejection of Claims 1, 6-15 and 17 Under 35 U.S.C. §103(a)

Claims 1, 6-15 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard (SecurSight: An architecture for secure information) in view of Hypponen (U.S. 6,986,050 B2), and further in view of Bathrick *et al.* (U.S. 5,825,300). Withdrawal of this rejection is requested for the following reasons. Brainard, Hyppopen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

> To reject claims in an application under §103, an examiner must show an unrebutted *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. This is achieved by providing a strong set of security credentials between a master entity such as a service and a remote entity such as a partner. In conjunction with the strong set of security credentials, a protocol is provided that acts as a package, wrapper or container to house the security credentials before delivery from the service to the partner to facilitate secure communications between the parties. In particular, independent claim 1 recites *a system and method for facilitating a computer a security connection between entities, comprising* ***a wrapper that packages credentials associated with resources of a service; and a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key****, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and the pass-phrase distributed separately from the credentials.* Brainard,

Hypponen and Bathrick, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Brainard relates to an architecture that secures access to network resources, while providing a smooth migration path from legacy authentication and authorization methods to a public key infrastructure. At page 6 of the Office Action, the Examiner concedes that Brainard does not teach such novel features. The Examiner attempts to compensate for the aforementioned deficiencies of Brainard with Hypponen and Bathrick *et al.* Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. A user is asked to enter a password and a passphrase, the system uses the passphrase to generate a cryptographic key, stores it in the system and uses it to encrypt and decrypt the data. Alternatively, Hypponen discloses the cryptographic key being derived independent of the password, with the key being encrypted using the passphase or using a second key derived using the passphase. However, the passphrase taught by Hypponen is used to generate a cryptographic key that allows access to encrypted data. On the contrary, the claimed invention generates a passphrase, a cryptographic wrapping key is generated from the pass-phase and this key is employed to generate the wrapper in which the credentials are wrapped. Thus, Hypponen is silent regarding ***a wrapper that packages credentials associated with resources of a service; and a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. The certifying authority generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. Nowhere does Bathrick *et al.* teach ***a wrapper that packages credentials associated with resources of a service, a pass phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as taught by applicants' subject claims.

In view of the above, Brainard, Hyppopen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is respectfully submitted that this rejection be withdrawn with respect to independent claim 1(and the claims that depend there from).

IV. Rejection of Claim 16 Under 35 U.S.C. §103(a)

Claim 16 is rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard in view of Hypponen further in view of Bathrick *et al.* further in view of Kay, *et al.* (U.S. 6,993,555 B2). Withdrawal of this rejection is requested for the following reasons. Claim 16 depends from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Kay *et al.* relates to a system for autonomously processing requests from remotely located users, using an instant messaging protocol, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claim 16 depends) be withdrawn.

V. Rejection of Claims 3-5 Under 35 U.S.C. §103(a)

Claims 3-5 are rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard in view of Hypponen, further in view of Bathrick *et al.* further in view of Rahman *et al.* (U.S. 7,114,080 B2). Withdrawal of this rejection is requested for the following reasons. Claims 3-5 depend from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Rahman *et al.* relates to a system that employs multiple computers outside a firewall and a password scheme that includes a one-time password and has biometric features, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claims 3-5 depend from) be withdrawn.

VI. Rejection of Claims 18 and 20 Under 35 U.S.C. §103(a)

Claims 18 and 20 are rejected under 35 U.S.C. §103(a) as being unpatentable over Epstein, *et al.* (U.S. 2002/0124064 A1) in view of Hardy, *et al.* (U.S. 5,222,135) further in view of Bathrick *et al.* Withdrawal of this rejection is requested for the following reasons. Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. Independent claim 18 recites *a method to facilitate a security connection between entities, comprising: generating a strong password; generating a pass-phrase;* ***wrapping the password cryptographically via the pass-phrase; storing the wrapped password in an executable****; and transmitting the executable and the pass-phrase to a system via different communications mediums.* Epstein *et al.*, Hardy *et al.* and Bathrick *et al.* are silent regarding such novel features.

Epstein *et al.* relates to a method to control a network through distributed control points. At page 10 of the Office Action, the Examiner contends that Epstein *et al.* teaches wrapping the password cryptographically via the pass phrase. Applicants' representative avers to the contrary. In accordance with the claimed invention, the system generates a pass phrase, which is employed to generate a cryptographic wrapping key. The wrapping key is then employed to cryptographically wrap or insulate the password in the wrapper or package. After the password has been placed in the wrapper, the pass phrase has to be entered to retrieve the credentials. At the cited portions, Epstein *et al.* discloses a pass phrase that has the one time key encoded within it. A control point is activated using the pass phrase. A new connection from the activated control point is received by using the one time key extracted from the pass phrase. Nowhere does Epstein *et al.* teach using the pass phrase to open the wrapper to access the password, and hence is silent regarding ***wrapping the password cryptographically via the pass-phrase*** as recited by the subject claims. The Examiner attempts to compensate for the aforementioned deficiencies of Epstein *et al.* with Hardy *et al.* and Bathrick *et al.*

Hardy *et al.* relates to a method for controlling the use of a data processing workstation by password. At the cited portions, Hardy *et al.* discloses storing an encrypted password in an executable and transmitting it. The password however, is not cryptographically wrapped via the pass phrase. Hence, Hardy *et al.* is silent regarding ***wrapping the password cryptographically via the pass-phrase; storing the wrapped password in an executable*** as recited by the subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. Bathrick *et al.* does not teach ***wrapping the password***

cryptographically via the pass-phrase; storing the wrapped password in an executable as recited by the subject claims.

In view of the above, Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is respectfully submitted that this rejection be withdrawn with respect to independent claim 18 (and the claims that depend there from).

VII. Rejection of Claims 21-26 Under 35 U.S.C. §103(a)

Claims 21-26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Epstein, *et al.* (U.S. 2002/0124064 A1) in view of Hardy, *et al.* (U.S. 5,222,135) further in view of Bathrick *et al.* (U.S. 5,825,300) further in view of Brainard (SecurSight: An architecture for secure information). Withdrawal of this rejection is requested for the following reasons. Claims 21-26 depend from independent claim 18. As discussed *supra*, Epstein *et al.*, Hardy *et al.* and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claim. Brainard relates to an architecture that secures access to network resources, while providing a smooth migration path from legacy authentication and authorization methods to a public key infrastructure, and does not make up for the deficiencies of Epstein *et al*, Hardy *et al.* and Bathrick *et al.* with respect to independent claim 18. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 18 (from which claims 21-26 depend from) be withdrawn.

VIII. Rejection of Claims 27-29 and 31-33 Under 35 U.S.C. §103(a)

Claims 27-29 and 31-33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rahman, *et al.* (U.S. 7,114,080 B2) in view of Nemovicher (U.S. 2002/0007453 A1). Withdrawal of this rejection is requested for the following reasons. Rahman *et al.*, and Nemovicher, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. Independent claim 27 recites *a computer executable system to facilitate a security relationship between parties, comprising: computer implemented means for generating a password****; computer implemented***

means for generating a pass-phrase*; computer implemented means for generating a package of credentials;* ***computer implemented means for storing the password separate from the package; computer implemented means for locking the package with the pass-phrase****; and computer implemented means for transmitting the package and the pass-phrase to a system via different communications mediums.* Independent claim 31 recites similar features. Rahman *et al.*, and Nemovicher are silent regarding such novel features.

Rahman *et al.* relates to a system that uses biometric features combined with a one-time password to generate cryptographic keys that are used for secure communication, authentication of remote users and accessing secured files. At page 14 of the Office Action, the Examiner concedes that Rahman *et al.* does not teach a pass phrase employed in connection with generation of cryptographic wrapping key, the pass phrase distributed separately from the credentials. The Examiner attempts to compensate for the aforementioned deficiencies of Rahman *et al.* with Nemovicher.

Nemovicher relates to a client server system for sending and receiving secure e-mail transmissions that are date stamped, virus scanned and authenticated at a centralized server. At the cited portions, Nemovicher discloses an e-mail message from a sender, along with a digital signature for authentication, being received by a server, the server decrypts the message, verifies it and adds another digital signature, encrypts the message with a one-time random key, and re-transmitts the secure message to a recipient who does not subscribe to the service. The one time random key is encrypted and packaged with the encrypted message form, a public key generated from a pass phrase (or password) taken from the saved sender e-mail message and both digital signatures, the package is attached to an e-mail message and sent to the recipient. The recipient can open the received package using the pass phrase (or password) obtained through separate communication channels from the sender. The system of Nemovitch packages the credentials and sends it to the recipient who uses the pass phrase to open the package, get the credentials and view the message. However, Nemovitch is silent regarding means for storing the password, and for locking the package with the pass phrase. Further, Nemovitch discloses a recipient who subscribes to the service, receiving the package and opening it with the encrypted private key. In that embodiment, the pass phrase is not transmitted via different communication mediums. Thus, Nemovitch does not teach ***computer implemented means for storing the password***

separate from the package; computer implemented means for locking the package with the pass-phrase as recited by the subject claims.

In view of the above, it is clear that Rahman *et al.*, and Nemovicher, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is requested that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731